

# Conditional probabilities and density operators in quantum modeling

John M. Myers

Gordon McKay Laboratory, Division of Engineering and Applied Sciences  
Harvard University, Cambridge, Massachusetts 02138

(Dated: 07 June 2005)

Based on a recent proof of free choices in linking equations to the experiments they describe, I clarify relations among some purely mathematical entities featured in quantum mechanics (probabilities, density operators, partial traces, and operator-valued measures), thereby allowing applications of these entities to the modeling of a wider variety of physical situations.

Conditional probabilities associated with projection-valued measures are expressed by introducing *conditional density operators*, identical in some but not all cases to the usual reduced density operators. By lifting density operators to the extended Hilbert space featured in Neumark's theorem, I show an obstacle to extending conditional density operators to arbitrary positive operator-valued measures (POVMs); however, tensor products of POVMs are compatible with conditional density operators.

By way of application, conditional density operators together with the free choice of probe particles allow the so-called postulate of state reductions to be replaced by a theorem. A second application demonstrates an equivalence between one form of quantum key distribution and another, allowing a formulation of individual eavesdropping attacks against transmitted-state BB84 to work also for entangled-state BB84.

PACS numbers: 03.65.Ta, 03.67.Dd

## I. INTRODUCTION

A recent proof confirms what to some will seem a commonplace: the equations of quantum mechanics are separated by a logical gap from their application to describing experiments with devices, so that choosing equations to describe devices involves an irreducible element of judgment [1]. This finding impacts a core question of interpretation: what does quantum mechanics describe [2]? Although a wide variety of interpretations accept the assumptions on which the proof depends, the proof tells us that quantum mechanics by itself describes nothing, but instead offers a mathematically articulated language that people speak to describe what they see or expect or think possible in experiments [3, 4].

With the recognition of a logical gap between the equations and experiments comes an opportunity to examine relations among some purely mathematical entities—probabilities, density operators, partial traces—separated out from the choices and judgments necessary to apply them to describing experiments. Based on this examination, I will show uses of *conditional density operators* defined in relation to the trace rule by which quantum mechanics generates probabilities from density operators and positive operator-valued measures.

The next section reviews the expression of joint and conditional probabilities by tensor products of projection-valued measures. Section III generalizes from projection-valued measures to positive operator-valued measures (POVMs) with a proposition that lifts density operators to an extended Hilbert space associated with Neumark's theorem. Diagrams show how tensor products of POVMs (but not generic operator products) express joint probabilities, leading to conditional density operators useful in modeling measurements of composite systems.

Section IV shows how choices in the application of quantum mathematics to the description of devices allows a single, discrete measure space to be applied in describing diverse situations. Section V offers two applications of the conditional probabilities and partial traces: (1) a demonstration that the use of reduced states in quantum mechanics requires no postulate about “effects of a measurement on a state”; and (2) a demonstration of the equivalence of two forms of quantum key distribution (QKD) [5], which I term “transmitted-state BB84” and “entangled-state BB84” [6] with the result that a known formulation [7] for studying individual eavesdropping attacks against transmitted-state BB84 applies also to entangled-state BB84.

## II. PROBABILITIES, OPERATOR-VALUED MEASURES, AND QUANTUM MODELING

By a probability measure I mean a completely additive set function [8], or, in more modern words, a positive measure [9, 10] of total measure 1. Let  $\Omega$  be a topological space; let  $\mathcal{M}(\Omega)$  be the  $\sigma$ -algebra of measurable subsets in  $\Omega$ , making  $\Omega$  into a measurable space. Let  $\mu$  denote any probability measure on a fixed  $\mathcal{M}(\Omega)$ . For any measurable sets  $X$  and  $Y$ , with  $\mu(Y) > 0$ , the conditional probability of  $X$  given  $Y$  is defined [8] as:

$$\mu(X|Y) \stackrel{\text{def}}{=} \mu(X \cap Y)/\mu(Y). \quad (2.1)$$

Let  $\mathcal{B}(\mathcal{H})$  denote the set of bounded, linear operators on a Hilbert space  $\mathcal{H}$ . With  $\mathcal{M}(\Omega)$  as above, a positive operator-valued measure (POVM) is any function

$$M : \mathcal{M}(\Omega) \rightarrow \mathcal{B}(\mathcal{H}) \quad (2.2)$$

satisfying: (1)  $M(\emptyset) = 0$ ,  $M(\Omega) = 1_{\mathcal{H}}$ ; (2) each  $M(X)$  is self-adjoint and non-negative; (3) if  $X \cap Y = \emptyset$  then  $M(X \cup Y) = M(X) + M(Y)$ ; and (4) for every  $|u\rangle, |v\rangle \in \mathcal{H}$ , the set function  $M_{u,v}$  defined by  $M_{u,v}(X) = \langle v|M(X)|u\rangle$  is a complex measure on  $\mathcal{M}(\Omega)$ .

A projection-valued measure, sometimes called a projective resolution of the identity [10], is a special case of a POVM, denoted here by  $E$  in place of  $M$ , that satisfies the above requirements, and, in addition:

$$\text{Each } E(X) \text{ is a self-adjoint projection (so } E^2(X) = E(X)); \quad (2.3)$$

$$E(X \cap Y) = E(X)E(Y). \quad (2.4)$$

Note that this last property implies

$$[E(X), E(Y)] \stackrel{\text{def}}{=} E(X)E(Y) - E(Y)E(X) = 0. \quad (2.5)$$

I take a density operator on  $\mathcal{H}$  to be any positive, self-adjoint trace-class operator  $\rho \in \mathcal{B}(\mathcal{H})$  such that  $\text{Tr}(\rho) = 1$ , where  $\text{Tr}$  denotes the trace [11]. If  $\rho$  is a density operator on  $\mathcal{H}$ , so is  $U\rho U^\dagger$  where  $U$  is any unitary operator on  $\mathcal{H}$ . For any POVM defined for  $\mathcal{M}(\Omega)$  and  $\mathcal{H}$ , along with any density operator  $\rho$  on  $\mathcal{H}$  and any unitary operator  $U$  on  $\mathcal{H}$ , a probability measure on  $\mathcal{M}(\Omega)$  is defined by

$$\mu(\rho, U, M; X) = \text{Tr}[U\rho U^\dagger M(X)]. \quad (2.6)$$

In the modeling of experiments one is interested in a family of such measures, corresponding to various choices of  $\rho$ ,  $U$ , and  $M$ . Often one skips the listing of these “parameters” and writes  $\text{Pr}(X)$  in place of  $\mu(\rho, U, M; X)$ . Feller speaks of  $\Omega$  as a “sample space” and of  $\mathcal{M}(\Omega)$  as “the set of events” [12], inviting us to think of a “probability that a sample point falls in an event set  $X$ ”; and, correspondingly, to think of  $\mu(X|Y)$  as a conditional probability that a sample point falls in  $X$  given that it falls in  $Y$ . (Without drawing a distinction between a sample point and an event, Dirac [13] speaks of a “result” while Peres [14] speaks of an “outcome.”)

In quantum physics we speak of a preparation of a state  $\rho$ , a time evolution  $U$ , and a measurement expressed by  $M$ . Quantum decision theory [15] adjoins to this story of “quantum probability” a “classical probability” in the choice of the state  $\rho$  prepared, making two kinds of events. To distinguish these kinds, I rename the event above a *measurement event* and join it to a *state event* expressing preparation of the state. States are usually thought of as selected from a discrete space of possible states, in which case the state event can be denoted simply by the state chosen, resulting in a compound event consisting of a measurement event  $X$  (as before) together with a state event  $\rho$ . The marginal probability for choosing  $\rho$  can be denoted  $\text{Pr}(\rho)$ . With this convention, decision problems are formulated in terms of a (joint) measure

$$\mu(U, M; \rho, X) = \text{Pr}(\rho)\text{Tr}[U\rho U^\dagger M(X)], \quad (2.7)$$

where on the left-hand side of the equation  $\rho$  has moved from the ‘parameter side’ of the semicolon to the ‘variable side.’ If  $U$  and  $M$  are understood, one can write  $\text{Pr}(\rho, X)$  in place of  $\mu(U, M; \rho, X)$ . (Models that go further by randomizing the choices of  $M$  and/or  $U$  can be found, but not in this report.)

By *quantum modeling* I mean stating probabilities in the form of Eqs. (2.6) or (2.7) (together with probabilities derived from these by Bayes’ rule) as mathematical language by which to ask questions and make statements pertaining

to a set of trials of devices in a laboratory experiment [1, 3]. Examples of devices are lasers, lenses, and detectors. In this language a trial is necessarily described as consisting of “preparing a state” and “measuring a state,” in some cases interspersing these with a temporal evolution  $U$ .

In quantum modeling, one speaks of various conditional probabilities, conditioned on whatever types of events are expressed in a model; hence there can be conditioning not only on *measurement events* but also on *state events*:

1. Understanding some  $\rho$ ,  $M$ , and  $U$ , one can speak of the conditional probability  $\Pr(X|Y)$  of a sample point being in measurement event set  $X$ , given it is in set  $Y$ .
2. Understanding some  $M$  and  $U$ , one can speak of the conditional probability of a measurement event  $X$ , given the state is  $\rho$ . For example, from Eq. (2.7) and the definition of a conditional probability, we see what in Eq. (2.6) appeared as a probability becomes in the context of decision theory a species of conditional probability:

$$\Pr(X|\rho) = \frac{\Pr(\rho, X)}{\Pr(\rho)} = \text{Tr}[U\rho U^\dagger M(X)]. \quad (2.8)$$

Variations on both of these appear below.

#### A. Conditional density operators for a single projection-valued measure

For the rest of this section and all of Sec. III, I subsume  $U\rho U^\dagger$  into  $\rho$ . By virtue of Eqs. (2.1), (2.4) and (2.5), conditional probabilities of a sample point being in one measurement event given that the point is in another measurement event fit in neatly with any single projection-valued measure  $E$ :

$$(\forall X, Y \in \mathcal{M}(\Omega) \text{ with } \Pr(Y) > 0) \quad \Pr(X|Y) = \frac{\text{Tr}[\rho E(X)E(Y)]}{\text{Tr}[\rho E(Y)]} = \frac{\text{Tr}[E(Y)\rho E(Y)E(X)]}{\text{Tr}[\rho E(Y)]}, \quad (2.9)$$

which allows us to define a “conditional density operator”

$$\rho|_Y \stackrel{\text{def}}{=} \frac{E(Y)\rho E(Y)}{\text{Tr}[\rho E(Y)]}, \quad (2.10)$$

with the property that

$$(\forall X) \quad \Pr(X|Y) = \text{Tr}[\rho|_Y E(X)]. \quad (2.11)$$

Similarly one constructs  $\rho|_X$  such that

$$(\forall Y) \quad \Pr(Y|X) = \text{Tr}[\rho|_X E(Y)]. \quad (2.12)$$

It is easy to check that the conditional density operators  $\rho|_Y$  and  $\rho|_X$  are non-negative, self-adjoint, and have unit trace. The expression of a conditional probability by a conditional density operator depends on the expression of a joint probability by a product of projections, as illustrated by the following commutative diagram (where commutative means that alternative ways to compose mappings arrive at the same thing):

$$\begin{array}{ccccc} X & \longmapsto & X \cap Y & \longleftarrow & Y \\ \downarrow & & \downarrow & & \downarrow \\ E(X) & \longmapsto & E(X)E(Y) & \longleftarrow & E(Y) \end{array} . \quad (2.13)$$

Diagram 1:  $E(X \cap Y) = E(X)E(Y)$ .

Although most of the conditional density operators to be introduced below are constructed using partial traces,  $\rho|_Y$  as defined by Eq. (2.10) involves no partial trace and so is not a reduced density operator, which shows that the concept of a conditional density operator is distinct from the concept of a reduced density operator.

**Note:** The conditional probabilities above are just probabilities that a measurement sample point that falls in a set  $Y$  also falls in a set  $X$ ; this has nothing to do with “consecutive measurements,” nor with so-called “state reductions” or “collapse of a wave function” postulated by Dirac [13] and von Neumann [11].

### B. Tensor products of projection-valued measures

Consider a special case that arises in the modeling of systems viewed as composites of subsystems  $A$  and  $B$ , so that

$$\begin{aligned}\Omega &= \Omega_A \times \Omega_B \quad (\text{cartesian product}), \\ \mathcal{H} &\equiv \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \quad (\text{tensor product}), \\ E &= E_A \otimes E_B \quad \text{with } E_A \text{ on } \mathcal{H}_A \text{ and } E_B \text{ on } \mathcal{H}_B, \\ \rho &= \rho_{AB} \in \mathcal{B}(\mathcal{H}_{AB}), \\ U &= \mathbf{1}_{AB}.\end{aligned}\tag{2.14}$$

The tensor product of projection-valued measures is defined by:

$$(\forall X_A \in \mathcal{M}(\Omega_A), Y_B \in \mathcal{M}(\Omega_B)) \quad (E_A \otimes E_B)(X_A \times Y_B) = E_A(X_A) \otimes E_B(Y_B).\tag{2.15}$$

Then we have

$$(X_A \times \Omega_B) \cap (\Omega_A \times Y_B) = (X_A \times Y_B),\tag{2.16}$$

$$(E_A \otimes E_B)[(X_A \times \Omega_B) \cap (\Omega_A \times Y_B)] = (E_A \otimes E_B)(X_A \times Y_B) = E_A(X_A) \otimes E_B(Y_B),\tag{2.17}$$

and the following diagram commutes:

$$\begin{array}{ccccccc} X_A & \mapsto & X_A \times \Omega_B & \mapsto & (X_A \times \Omega_B) \cap (\Omega_A \times Y_B) & \hookleftarrow & \Omega_A \times Y_B & \hookleftarrow & Y_B \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ E_A(X_A) & \mapsto & E_A(X_A) \otimes \mathbf{1}_B & \mapsto & E_A(X_A) \otimes E_B(Y_B) & \hookleftarrow & \mathbf{1}_A \otimes E_B(Y_B) & \hookleftarrow & E_B(Y_B) \end{array}.\tag{2.18}$$

Diagram 2: Tensor product of projection-valued measures.

For this specialization of Diagram 1, it follows from Eqs. (2.9) and (2.17) that

$$\begin{aligned}\Pr(X_A|Y_B) &\equiv \Pr(X_A \times \Omega_B | \Omega_A \times Y_B) \\ &= \frac{\text{Tr}_{AB}\{[\mathbf{1}_A \otimes E_B(Y_B)]\rho_{AB}[\mathbf{1}_A \otimes E_B(Y_B)](E_A(X_A) \otimes \mathbf{1}_B)\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y_B)]\}},\end{aligned}\tag{2.19}$$

where the subscript  $AB$  on the trace indicates the trace over  $\mathcal{H}_{AB}$ . From this follow two distinct ways to define a conditional density operator:

1. Eq. (2.12) implies:

$$\Pr(X_A|Y_B) = \text{Tr}_{AB}[\rho_{AB}^{(1)}|_{Y_B}(E_A(X_A) \otimes \mathbf{1}_B)],\tag{2.20}$$

with

$$\rho_{AB}^{(1)}|_{Y_B} \stackrel{\text{def}}{=} \frac{[\mathbf{1}_A \otimes E_B(Y_B)]\rho_{AB}[\mathbf{1}_A \otimes E_B(Y_B)]}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y_B)]\}}.\tag{2.21}$$

2. The alternative definition takes advantage of partial traces to obtain a conditional density operator as a reduced density operator:

$$\Pr(X_A|Y_B) = \frac{\text{Tr}_A \text{Tr}_B\{[\mathbf{1}_A \otimes E_B(Y_B)]\rho_{AB}[\mathbf{1}_A \otimes E_B(Y_B)](E_A(X_A) \otimes \mathbf{1}_B)\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y_B)]\}},\tag{2.22}$$

which, with  $X \equiv X_A$  and  $Y \equiv Y_B$  understood, can be written with less clutter as

$$\begin{aligned}\Pr(X|Y) &= \frac{\text{Tr}_A \text{Tr}_B\{[\mathbf{1}_A \otimes E_B(Y)]\rho_{AB}[\mathbf{1}_A \otimes E_B(Y)](E_A(X) \otimes \mathbf{1}_B)\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y)]\}} \\ &= \text{Tr}_A[\rho_A^{(2)}|_Y(E_A(X) \otimes \mathbf{1}_B)],\end{aligned}\tag{2.23}$$

with

$$\begin{aligned}
\rho_A^{(2)}|_Y &\stackrel{\text{def}}{=} \frac{\text{Tr}_B\{[\mathbf{1}_A \otimes E_B(Y)]\rho_{AB}[\mathbf{1}_A \otimes E_B(Y)]\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y)]\}} \\
&= \frac{\text{Tr}_B\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y)]\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes E_B(Y)]\}}.
\end{aligned} \tag{2.24}$$

I stretch notation to allow  $\text{Tr}_A$  to indicate either the partial trace over the factor  $\mathcal{H}_A$  of the tensor-product Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  or the trace over just the Hilbert space  $\mathcal{H}_A$ . Properties of the partial trace used in these equations are reviewed in Appendix A; for example, Eq. (A10) assures us that the last expression in Eq. (2.24) is a self-adjoint operator on  $\mathcal{H}_A$ .

When this mathematics of tensor products is applied to model a measurement event viewed as a rectangle  $X_A \times Y_B$ , it is convenient to speak of  $X_A$  and  $Y_B$  separately as pertaining to *components* of the measurement event.

### III. POSITIVE OPERATOR-VALUED MEASURES AND CONDITIONAL PROBABILITIES

The diagram (2.13) fails for generic POVMs, but the specialization to tensor-products holds for POVMs. How this works can be seen from Neumark's theorem, along with a corollary developed below.

#### A. Neumark's theorem

Suppose a Hilbert space  $\mathcal{H}$  is a subspace of a Hilbert space  $\mathcal{H}^+$ . Let  $E^+ : \mathcal{M}(\Omega) \rightarrow \mathcal{B}(\mathcal{H}^+)$  be any projection-valued measure on  $\mathcal{H}^+$ , and let  $Q \in \mathcal{B}(\mathcal{H}^+)$  be the orthogonal (hence self-adjoint) projection on  $\mathcal{H}$ . (Although consistency calls for writing this as  $Q^+$ , to avoid clutter I write just  $Q$ .) Define a POVM  $(QE^+Q)_\mathcal{H} : \mathcal{M}(\Omega) \rightarrow \mathcal{B}(\mathcal{H})$  by

$$(\forall X \in \mathcal{M}(\Omega)) \quad (QE^+Q)_\mathcal{H}(X) = (QE^+(X)Q)_\mathcal{H}, \tag{3.1}$$

where  $\mathcal{H}$  as a subscript denotes the restriction of an operator to  $\mathcal{H}$ .

Neumark [16, 17] proved that all POVMs can be expressed this way: for any POVM  $M$  on any Hilbert space  $\mathcal{H}$ , there exists a Hilbert space  $\mathcal{H}^+$  containing  $\mathcal{H}$  as a subspace, and there exists a projective resolution of the identity  $E^+ : \mathcal{M}(\Omega) \rightarrow \mathcal{B}(\mathcal{H}^+)$  such that  $M = (QE^+Q)_\mathcal{H}$ .

#### B. Lifting the trace rule to $\mathcal{H}^+$

It is instructive to lift the trace rule to the extended Hilbert space  $\mathcal{H}^+$ . When we view  $\mathcal{H}$  as a subspace of  $\mathcal{H}^+$ , we see any vector  $|\psi\rangle \in \mathcal{H}$  as a vector  $|\psi\rangle \oplus |0\rangle^\perp$  in  $\mathcal{H}^+$ , where  $|0\rangle^\perp$  denotes the 0-vector in  $\mathcal{H}^\perp$ . Correspondingly, we view any operator  $A \in \mathcal{B}(\mathcal{H})$  as an operator  $A \oplus \mathbf{0}^\perp \in \mathcal{B}(\mathcal{H}^+)$ , where  $\mathbf{0}^\perp$  is the zero operator on  $\mathcal{H}^\perp$ . With  $Q \in \mathcal{B}(\mathcal{H}^+)$  the orthogonal projection onto  $\mathcal{H}$  as above, useful elementary facts are

$$\begin{aligned}
(\forall A, B \in \mathcal{B}(\mathcal{H}))(\forall C^+, D^+ \in \mathcal{B}(\mathcal{H}^+)) \\
Q(A \oplus \mathbf{0}^\perp)Q &= A \oplus \mathbf{0}^\perp,
\end{aligned} \tag{3.2}$$

$$QC^+Q = (QC^+Q)_\mathcal{H} \oplus \mathbf{0}^\perp, \tag{3.3}$$

$$(A \oplus \mathbf{0}^\perp)(B \oplus \mathbf{0}^\perp) = (AB) \oplus \mathbf{0}^\perp, \tag{3.4}$$

$$\text{Tr}^+(A \oplus \mathbf{0}^\perp) = \text{Tr}(A), \tag{3.5}$$

where  $\text{Tr}$  denotes the trace on  $\mathcal{H}$  and  $\text{Tr}^+$  denotes the trace on  $\mathcal{H}^+$ . From these equations follows

**Lemma:**

$$\begin{aligned}
\text{Tr}^+[(A \oplus \mathbf{0}^\perp)C^+] &= \text{Tr}^+[Q(A \oplus \mathbf{0}^\perp)QC^+] \\
&= \text{Tr}^+[(A \oplus \mathbf{0}^\perp)QC^+Q]
\end{aligned}$$

$$\begin{aligned}
&= \text{Tr}^+ \{ (A \oplus \mathbf{0}^\perp) [(QC^+Q)_\mathcal{H} \oplus \mathbf{0}^\perp] \} \\
&= \text{Tr}^+ [A(QC^+Q)_\mathcal{H} \oplus \mathbf{0}^\perp] \\
&= \text{Tr} [A(QC^+Q)_\mathcal{H}].
\end{aligned} \tag{3.6}$$

Letting  $A$  be  $\rho$  and  $C^+$  be  $E^+(X)$  yields

**Proposition:**

$$(\forall \rho) (\forall X \in \mathcal{M}(\Omega)) \quad \text{Pr}(X|\rho) \equiv \text{Tr}[\rho M(X)] = \text{Tr}^+[(\rho \oplus \mathbf{0}^\perp) E^+(X)]. \tag{3.7}$$

Eq. (3.7) allows the trace rule for any given single POVM to be lifted to  $\mathcal{H}^+$ , as illustrated in the commutative diagram

$$\begin{array}{ccc}
E^+(X) & & (\rho \oplus \mathbf{0}^\perp) \in \mathcal{B}(\mathcal{H}^+) \\
\swarrow & & \swarrow \\
Q, |\mathcal{H} \downarrow & \text{Tr}^+[(\rho \oplus \mathbf{0}^\perp) E^+(X)] & \downarrow Q, |\mathcal{H} \\
& = & \\
& \text{Tr}[\rho M(X)] & \\
\swarrow & & \swarrow \\
M(X) & & \rho \in \mathcal{B}(\mathcal{H})
\end{array} . \tag{3.8}$$

Diagram 3: Lifting of the trace rule to  $\mathcal{H}^+$  via Neumark's theorem.

### C. Obstacle to expressing conditional probabilities with POVMs

The desire to extend the diagram engendered by Proposition (3.7) to  $\text{Pr}(X \cap Y|\rho)$  for the set intersection  $X \cap Y$  encounters the following obstacle:

$$\begin{array}{ccccc}
E^+(X) & \longmapsto & E^+(X \cap Y) = E^+(X) E^+(Y) & \longleftarrow & E^+(Y) \\
\downarrow Q, |\mathcal{H} & & \downarrow & & \downarrow \\
& & M(X \cap Y) = [QE^+(X)E^+(Y)Q]_\mathcal{H} & & \\
& & \neq & & \\
M(X) = [QE^+(X)Q]_\mathcal{H} & \longmapsto & M(X)M(Y) = [QE^+(X)Q]_\mathcal{H} [QE^+(Y)Q]_\mathcal{H} & \longleftarrow & M(Y) = [QE^+(Y)Q]_\mathcal{H}
\end{array} . \tag{3.9}$$

Diagram 4: Obstacle to lifting of product of POVMs.

Because

$$[QE^+(X)E^+(Y)Q]_\mathcal{H} \neq [QE^+(X)Q]_\mathcal{H} [QE^+(Y)Q]_\mathcal{H}, \tag{3.10}$$

we find that except in uninteresting special cases

$$M(X \cap Y) \neq M(X)M(Y). \tag{3.11}$$

Correspondingly, efforts to define reduced states corresponding to a measurement modeled by  $M(X)$  followed by a measurement modeled by  $M(Y)$  encounter conceptual difficulties, touched on by Braunstein and Caves [18] and discussed below in connection with probes.

### D. Tensor products of POVMs

The obstacle to operator products of POVMs is no impediment to tensor products. Consider a POVM  $M_A : \mathcal{M}(\Omega_A) \rightarrow \mathcal{B}(\mathcal{H}_A)$  and another POVM  $M_B : \mathcal{M}(\Omega_B) \rightarrow \mathcal{B}(\mathcal{H}_B)$ . By Neumark's theorem, both of these POVMs can be expressed as restrictions of projections of projection-valued measures on the respective extended Hilbert spaces:  $E_A^+ : \mathcal{M}(\Omega_A) \rightarrow \mathcal{B}(\mathcal{H}_A^+)$  and  $E_B^+ : \mathcal{M}(\Omega_B) \rightarrow \mathcal{B}(\mathcal{H}_B^+)$ , respectively. Let  $Q_A \in \mathcal{B}(\mathcal{H}_A^+)$  be the orthogonal (hence self-adjoint) projection on  $\mathcal{H}_A$ , and similarly  $Q_B \in \mathcal{B}(\mathcal{H}_B^+)$ . Because a tensor product of projections is a projection, Diagram 2 for the extended Hilbert spaces extends downward, via  $Q_A$  and  $Q_B$  followed by reductions, to  $\mathcal{H}$ . The neat thing here is that

$$(Q_A \otimes Q_B)(E_A^+ \otimes E_B^+)(Q_A \otimes Q_B) = (Q_A E_A^+ Q_A) \otimes (Q_B E_B^+ Q_B), \quad (3.12)$$

the restriction of which to the subspace  $\mathcal{H}_A \otimes \mathcal{H}_B$  is just  $M_A \otimes M_B$ ; i.e. we have

$$\begin{aligned} M_A \otimes M_B &= [Q_A E_A Q_A \otimes Q_B E_B Q_B]|_{\mathcal{H}_{BA}} \\ &= [(Q_A \otimes Q_B)(E_A \otimes E_B)(Q_A \otimes Q_B)]|_{\mathcal{H}_{BA}}. \end{aligned} \quad (3.13)$$

Thus we arrive at the diagram:

$$\begin{array}{ccccccc} E_A^+ & \rightarrow & E_A^+ \otimes \mathbf{1}_B & \rightarrow & E_A^+ \otimes E_B^+ & \leftarrow & \mathbf{1}_A \otimes E_B^+ \leftarrow E_B^+ \\ Q_A, |_{\mathcal{H}_A} & \downarrow & \downarrow & & \downarrow & & \downarrow Q_B, |_{\mathcal{H}_B} \\ M_A & \rightarrow & M_A \otimes \mathbf{1}_B & \rightarrow & M_A \otimes M_B & \leftarrow & \mathbf{1}_A \otimes M_B \leftarrow M_B \end{array} \quad (3.14)$$

Diagram 5: Tensor product of POVMs.

Because this shows

$$(M_A \otimes M_B)[(X_A \times \Omega_B) \cap (\Omega_A \times Y_B)] = M_A(X_A) \otimes M_B(Y_B), \quad (3.15)$$

Eqs. (2.19)–(2.23) hold also for non-projective POVMs; for instance, Eq. (2.23) becomes (with the understanding  $X \equiv X_A$  and  $Y \equiv Y_B$ ):

$$\begin{aligned} \Pr(X|Y) &= \frac{\text{Tr}_{AB}[M_A(X) \otimes M_B(Y)]\rho_{AB}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)]\}} \\ &= \frac{\text{Tr}_A \text{Tr}_B\{[\mathbf{1}_A \otimes M_B(Y)]\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)](M_A(X) \otimes \mathbf{1}_B)\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)]\}} \\ &= \text{Tr}_A[\rho_A|_Y M_A(X)], \end{aligned} \quad (3.16)$$

with

$$\rho_A|_Y \stackrel{\text{def}}{=} \frac{\text{Tr}_B\{[\mathbf{1}_A \otimes M_B(Y)]\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)]\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)]\}} = \frac{\text{Tr}_B\{\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)]\}}{\text{Tr}_{AB}\{\rho_{AB}[\mathbf{1}_A \otimes M_B(Y)]\}}. \quad (3.17)$$

### E. Tensor products of families of POVMs

Instead of considering a single POVM on  $\mathcal{H}_A$  and a single POVM on  $\mathcal{H}_B$ , we consider now two indexed families of POVMs,  $M_{A,\alpha}$  and  $M_{B,\beta}$ . Then Diagram 5 threatens to become decorated with these indices in a curiously asymmetric way, because the proof of Neumark's theorem presents  $\mathcal{H}_B$  not as a  $\beta$ -independent subspace of  $\mathcal{H}_B^+$ , but as one that varies with  $\beta$ .

The following corollary restores symmetry to the distribution of indices and justifies lifting not just one POVM but any family of POVMs to a single extended Hilbert space related to the base space by a single (index-independent) orthogonal projection.

**Corollary to Neumark's theorem:** Given a fixed Hilbert space  $\mathcal{H}$  and a fixed  $\sigma$ -algebra  $\mathcal{M}(\Omega)$  of measurable sets, together with any family of POVMs  $M_\beta : \mathcal{M}(\Omega) \rightarrow \mathcal{B}(\mathcal{H})$  (indexed by  $\beta$ ); then there is a single extended Hilbert space  $\mathcal{H}^+$  containing  $\mathcal{H}$  as a subspace and a single  $Q \in \mathcal{B}(\mathcal{H}^+)$ , the orthogonal projection on  $\mathcal{H}$ , along with a family of projection-valued measures  $E_\beta^+$  on  $\mathcal{H}^+$ , such that

$$(\forall \beta)(\exists E_\beta^+) \quad M_\beta = [QE_\beta^+Q]_{\mathcal{H}}. \quad (3.18)$$

*Proof sketch:* The proof of Neumark's theorem in [17] (and also in [16]) deals with each POVM of a family one at a time, so to speak: it constructs an extended Hilbert space  $\mathcal{H}^+$  that depends on  $\mathcal{M}(\Omega)$  but is independent of  $\beta$ ; then  $\mathcal{H}$  is mapped isomorphically onto a subspace that I denote  $\tilde{\mathcal{H}}_\beta \subset \mathcal{H}^+$  that depends on  $\beta$ ; implicit in the proof is an isomorphism carrying each density operator  $\rho \in \mathcal{B}(\mathcal{H})$  to  $\tilde{\rho}_\beta \in \mathcal{B}(\tilde{\mathcal{H}}_\beta)$ ; this works in such a way that  $E^+$  is independent of  $\beta$ . We want to swap these dependencies, to make  $\tilde{\mathcal{H}}$  independent of  $\beta$  in exchange for allowing a  $\beta$ -dependent  $E_\beta^+$ . I claim this works as follows. Pick any value of  $\beta$ , and call it 0; for this value of  $\beta$ ,  $\mathcal{H}$  is mapped isomorphically onto  $\tilde{\mathcal{H}}_0$ . For any value of  $\beta$  there exists a unitary transform  $U_\beta^+ \in \mathcal{B}(\mathcal{H}^+)$ , such that  $\tilde{\rho}_\beta \oplus \tilde{\mathbf{0}}_\beta^\perp = U_\beta^+(\rho \oplus \mathbf{0}^\perp)U_\beta^\dagger$ . From this and Proposition (3.7) it follows that

$$\begin{aligned} (\forall \beta, X) \quad \text{Tr}[\rho M_\beta(X)] &= \text{Tr}^+[E^+(X)(\tilde{\rho}_\beta + \tilde{\mathbf{0}}_\beta^\perp)] \\ &= \text{Tr}^+[U_\beta^+(\rho + \mathbf{0}^\perp)U_\beta^{\dagger\dagger}E^+(X)] \\ &= \text{Tr}^+[(\rho + \mathbf{0}^\perp)U_\beta^{+\dagger}E^+(X)U_\beta^+] \\ &= \text{Tr}^+[(\rho + \mathbf{0}^\perp)E_\beta^+(X)], \end{aligned} \quad (3.19)$$

where we define  $E_\beta^+(X) \stackrel{\text{def}}{=} U_\beta^{+\dagger}E^+(X)U_\beta^+$ . Equation (3.19) and Lemma (3.6) imply that for an orthogonal projection  $Q$  onto  $\tilde{\mathcal{H}}$ , independent of  $\beta$ ,  $(\forall \beta, X, \rho) \quad \text{Tr}[\rho M_\beta(X)] = \text{Tr}[\rho(QE_\beta^+(X)Q)_{\tilde{\mathcal{H}}}]$ , from which the conclusion of the corollary follows.  $\square$

A simple example in finite dimensions occurs in [19], where a plane on which a POVM is defined is embedded in a  $\beta$ -dependent way in a three space equipped with a fixed projection-valued measure defined by three mutually orthogonal basis vectors. As in the corollary, one can just as well hold the plane fixed and rotate the basis vectors.

We apply this as follows. Consider a family of POVMs indexed by  $\alpha$ ,  $M_{A,\alpha} : \mathcal{M}(\Omega_A) \rightarrow \mathcal{B}(\mathcal{H}_A)$ , along with another family of POVMs indexed by  $\beta$ ,  $M_{B,\beta} : \mathcal{M}(\Omega_B) \rightarrow \mathcal{B}(\mathcal{H}_B)$ . By the corollary, we translate Diagram 5 into a diagram for these families. For all  $\alpha, \beta$  we have:

$$\begin{array}{ccccccc} E_{A,\alpha}^+ & \rightarrow & E_{A,\alpha}^+ \otimes \mathbf{1}_B & \rightarrow & E_{A,\alpha}^+ \otimes E_{B,\alpha}^+ & \leftarrow & \mathbf{1}_A \otimes E_{B,\beta}^+ \leftarrow E_{B,\alpha}^+ \\ Q_A, |\mathcal{H}_A & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & Q_B, |\mathcal{H}_B \\ M_{A,\alpha} & \rightarrow & M_{A,\alpha} \otimes \mathbf{1}_B & \rightarrow & M_{A,\alpha} \otimes M_{B,\beta} & \leftarrow & \mathbf{1}_A \otimes M_{B,\beta} \leftarrow M_{B,\beta} \end{array} \quad (3.20)$$

Diagram 6: Tensor product of POVMs of two families.

By the corollary, we have a diagram in which  $Q_A$  and  $Q_B$  are independent of the indices  $\alpha, \beta$ .

#### IV. APPLYING QUANTUM PROBABILITIES TO DESCRIPTIONS OF DEVICES

Designs for systems of devices often start with models expressed in simplified equations; quantum cryptography is a case in point. Implementing a design inspired by equations entails arranging devices—lasers, detectors, counters—so that measured device behavior accords with properties expressed in the equations. Experience teaches that the devices work as desired only when nudged in ways unexpressed by the starting equations. To support this nudging, one ends up with layers of more detailed equations, needed for instance in order to design feedback loops that compensate for various drifts. Whatever details we undertake to model, we face choices. For example, in an experiment with pulsed light, if we assume there are no memory effects in the light detectors, we can implement the state preparation for



a trial by generating a single light pulse, while to study memory effects in detectors, we must implement the state preparation for a trial by generating a sequence of pulses [3]. When the equations used in modeling are equations in the language of quantum mechanics, different choices are expressed by different probability distributions stemming from different density operators and different positive operator-valued measures (POVMs), along with different choices of a measure space.

### A. Choice of measure space

To use a measure space as part of a quantum model of devices, one needs, somehow, to link parameters—frequencies, positions, times—by which one speaks in the laboratory of light pulses to the measure space. Several things complicate this linking. First, no single-frequency light state is an element of any separable Hilbert space. Second are laboratory facts (filters spill over, light diffracts, signal times are fuzzy). In modeling these facts, we need detection operators that are correspondingly unsharp in relation to the same parameters. Third, the specification of a measure space in terms of physical parameters depends on the layer of detail, and this impedes comparisons of models across different layers of detail. These complications are eased by adapting a trick from quantum decision theory, in which POVMs are defined not with respect to an arbitrary measure space but only for a discrete measure space, the elements of which are thought of not in terms of physical parameters but as possible actions to take in response to a measurement event.

So far the measure spaces appearing in this report have been arbitrary, i.e., without any additional constraints. They allow for real metric spaces needed to deal with continuous spectra of hermitian detection operators, and these measure spaces necessarily involve the physical parameters of the spectrum. We can preserve the capacity to deal with these parameters when we must, while sidestepping their complications when we can: the trick is to link arbitrary measure spaces to discrete measure spaces adapted from quantum decision theory [14, 15]. In quantum decision theory, a POVM is defined not with reference to a general measure space but as a countable set of detection operators  $M(j)$  that sum to 1. One can imagine the measurement result displayed by lighting up just one of a row of lamps, indexed by  $j$ . The context is one of action: “if light  $j$  goes on, do  $X_j$ .” To link this to a general measure space  $\Omega$ , we model an act of measuring not by a full POVM, but by a countable set of detection operators  $M(\Omega_j)$ , where for  $j = 1, 2, \dots$ , the  $\Omega_j$  are mutually disjoint subsets that cover  $\Omega$ . When we have in mind a mapping from natural numbers to measurable sets of some measure space  $\Omega$ , we can abbreviate  $M(\Omega_j)$  by  $M(j)$ . This abbreviation establishes a relation among detection operators at different levels of detail with distinct measure spaces  $\Omega$  and  $\Omega'$  by relating say  $M(\Omega_j)$  and  $M(\Omega'_j)$  to the same decision-oriented event  $j$ . By this linking of any arbitrary measure space to the natural numbers as a single discrete measure space, we make universally applicable the notion of a family of POVMs defined on that discrete measure space.

## V. TWO APPLICATIONS OF CONDITIONAL PROBABILITIES

Here are two applications of conditional probabilities as discussed above, the first conceptual, the second concrete.

### A. Sequences of probes in place of “consecutive measurements”

Tensor-product spaces are well suited to the modeling of the interaction of a particle with a succession of probes, followed by measurement of the probes, and in this connection a variety of conditional density operators can be useful. For example, express the particle to be probed by a density operator  $\rho_0 \in \mathcal{B}(\mathcal{H}_0)$ , and express probe  $j$ ,  $j = 1, 2, \dots$ , prior to its interaction with the particle by a density operator  $\rho_j \in \mathcal{B}(\mathcal{H}_j)$ . After a succession of interactions (shown in Fig. 1), expressed by unitary operators  $U_{0j} \in \mathcal{B}(\mathcal{H}_0 \otimes \mathcal{H}_j)$ , the probes are measured, as expressed by POVMs  $M_j : \mathcal{M}(\Omega_j) \rightarrow \mathcal{B}(\mathcal{H}_j)$  on the respective Hilbert spaces  $\mathcal{H}_j$ . For two probes, this procedure yields for the joint probability of components  $X_j$  of the measurement event:

$$\begin{aligned} \Pr(X_1, X_2) &= \text{Tr}_{012} \left( M_2(X_2) M_1(X_1) U_{02} \{ [U_{01}(\rho_0 \otimes \rho_1) U_{01}^\dagger] \otimes \rho_2 \} U_{02}^\dagger \right) \\ &= \text{Tr}_{02} [M_2(X_2) U_{02}(\sigma_0|_{X_1} \otimes \rho_2) U_{02}^\dagger], \end{aligned} \quad (5.1)$$

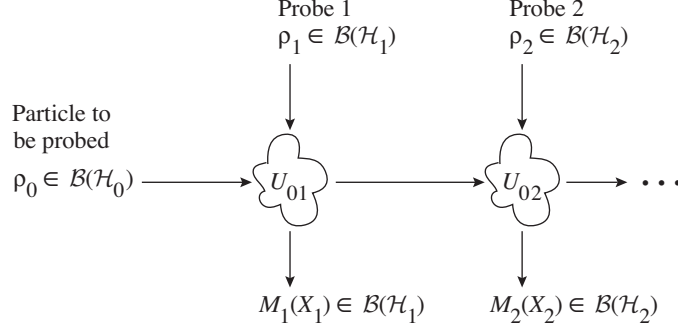


FIG. 1: Particle  $\rho_0$  undergoing successive interactions with probes  $\rho_1, \rho_2, \dots$

where

$$\sigma_0|_{X_1} = \text{Tr}_1[M(X_1)U_{01}(\rho_0 \otimes \rho_1)U_{01}^\dagger]. \quad (5.2)$$

The corresponding conditional probability of  $X_2$  given  $X_1$  is

$$\Pr(X_2|X_1) = \text{Tr}_{02}[M_2(X_2)U_{02}(\rho_0|_{X_1} \otimes \rho_2)U_{02}^\dagger], \quad (5.3)$$

where  $\rho_0|_{X_1}$  is the (normalized) conditional density operator engendered by the scaled conditional density operator  $\sigma_0|_{X_1}$ :

$$\rho_0|_{X_1} \stackrel{\text{def}}{=} \frac{\sigma_0|_{X_1}}{\text{Tr}_{02} \sigma_0|_{X_1}}. \quad (5.4)$$

For three probes, this procedure yields for the joint probability of components  $X_j$  of the measurement event:

$$\begin{aligned} \Pr(X_1, X_2, X_3) &= \text{Tr}_{023} \left[ M_3(X_3)M_2(X_2)U_{03} \left( [U_{02}(\sigma_0|_{X_1} \otimes \rho_2)U_{02}^\dagger] \otimes \rho_3 \right) U_{03}^\dagger \right] \\ &= \text{Tr}_{03} [M_3(X_3)U_{03}(\sigma_0|_{X_1, X_2} \otimes \rho_3)U_{03}^\dagger], \end{aligned} \quad (5.5)$$

where  $\sigma_0|_{X_1}$  is given in Eq. (5.2) and

$$\sigma_0|_{X_1, X_2} = \text{Tr}_2[M(X_2)U_{02}(\sigma_0|_{X_1} \otimes \rho_2)U_{02}^\dagger]. \quad (5.6)$$

Corresponding to these equations, we find for the conditional probabilities

$$\Pr(X_2, X_3|X_1) = \text{Tr}_{023} \left[ M_3(X_3)M_2(X_2)U_{03} \left( [U_{02}(\rho_0|_{X_1} \otimes \rho_2)U_{02}^\dagger] \otimes \rho_3 \right) U_{03}^\dagger \right], \quad (5.7)$$

$$\Pr(X_3|X_1, X_2) = \text{Tr}_{03} [M_3(X_3)U_{03}(\rho_0|_{X_1, X_2} \otimes \rho_3)U_{03}^\dagger], \quad (5.8)$$

where each conditional density operator is defined as usual by dividing a corresponding scaled conditional density operator by its trace.

Recognizing freedom to invoke probes such as these in modeling measurements has been shown to make the notion of repeated measurements unnecessary in formulating the mathematics of quantum mechanics in terms of projection-valued measures: a pair of successive measurements can be subsumed into a single measurement involving a succession of interactions of probes [1]. By virtue of Neumark's theorem and the corollary above which makes it applicable to a family of POVMs, this now generalizes to POVMs. Once freedom to invoke probes is accepted, there is no place nor any need in the logic of quantum mechanics for a postulate pertaining to consecutive measurements. In particular, notwithstanding the efforts of Dirac [13] and von Neumann [11] and others [20, 21] concerning consecutive measurements, there is no place for a postulate of so-called "state reductions."

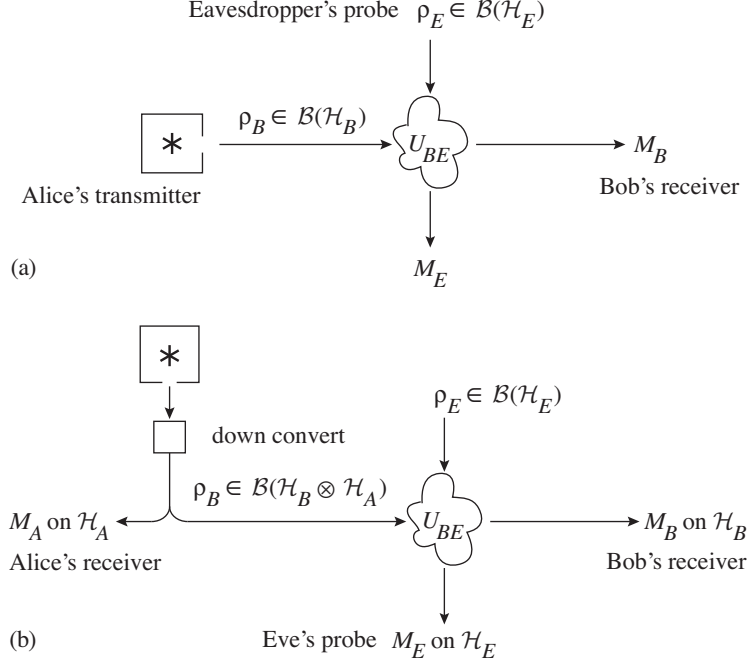


FIG. 2: (a) Transmitted-state QKD. (b) Entangled-state QKD.

### B. Example from quantum cryptography

Models of quantum key distribution (QKD) subject to individual eavesdropping attacks [5, 7] posit a sequence of trials, one trial for each raw key bit. The popular key protocol BB84 [6] has two versions, “transmitted-state” (Fig. 2a) and “entangled-state” (Fig. 2b). Transmitted-state BB84 calls at each trial for Alice to prepare at random one of four light states  $\rho_B(i)$ ,  $i = 1, \dots, 4$ , with prior probabilities  $\zeta_i$ ; these states, subject to probing by Eve, are detected by Bob. Entangled-state BB84 calls for Alice to prepare a single polarization-entangled light state  $\rho_{BA}$  that propagates to both her own detectors and to Bob’s detectors, again with the propagation to Bob subject to probing by Eve. Here I develop a relation that enables one to formulate individual attacks against the seemingly more complicated entangled-state BB84 in the same way as individual attacks against transmitted-state BB84.

The formulation by Slutsky *et al.* [7] for transmitted-state BB84 holds for general light states defined in [22, 23], not just the simplified states for which they carried through their analysis. As discussed in detail in [22, 24], all the probabilities pertinent to key distribution in the face of an individual eavesdropping attack against transmitted-state BB84 stem from  $\zeta_i$  together with the trace rule applied to a quantum state on a tensor-product space  $\mathcal{H}_E \otimes \mathcal{H}_B$ , where  $\mathcal{H}_B$  is a Hilbert space of light modes transmitted to Bob and  $\mathcal{H}_E$  is the Hilbert space of Eve’s probe. These probabilities have the form

$$\Pr(X_E, Y_B, \rho_B(i)) = \zeta_i \text{Tr}_{EB}[M_E(X_E)M_B(Y_B)U_{EB}(\rho_E \otimes \rho_B)U_{EB}^\dagger], \quad (5.9)$$

where  $U_{EB}$  represents an arbitrary unitary interaction chosen by Eve between her probe  $\rho_E$  and Bob’s light state  $\rho_B$ .

In models of entangled-state BB84, there are no prior probabilities  $\zeta_i$ ; instead, the Hilbert space involves three factors  $\mathcal{H}_E \otimes \mathcal{H}_B \otimes \mathcal{H}_A$ , where  $\mathcal{H}_A$  is the Hilbert space for light detected by Alice. At each trial Eve prepares a probe  $\rho_E$  as before, but now Alice prepares an entangled state  $\rho_{BA} \in \mathcal{B}(\mathcal{H}_B \otimes \mathcal{H}_A)$ . With  $U_{EB}$  as in transmitted-state BB84, the probabilities pertinent to key distribution in the face of an individual eavesdropping attack against entangled-state BB84 are just

$$\Pr(X_E, Y_B, Z_A) = \text{Tr}_{EBA}[M_E(X_E)M_B(Y_B)M_A(Z_A)U_{EB}(\rho_E \otimes \rho_{BA})U_{EB}^\dagger], \quad (5.10)$$

which looks significantly different from Eq. (5.9); however, by the partial trace manipulations of Appendix A, in

particular Eq. (A21), this last equation becomes

$$\Pr(X_E, Y_B, Z_A) = \text{Tr}_{EB}\{M_E(X_E)M_B(Y_B)U_{EB}[\rho_E \otimes \text{Tr}_A(M_A(Z_A)\rho_{BA})]U_{EB}^\dagger\}. \quad (5.11)$$

This implies the following probability for Alice's component  $Z_A$  of a measurement event (regardless of Bob's and Eve's):

$$\begin{aligned} \Pr(Z_A) &= \text{Tr}_{EB}\{U_{EB}[\rho_E \otimes \text{Tr}_A(M_A(Z_A)\rho_{BA})]U_{EB}^\dagger\} \\ &= \text{Tr}_{EB}[\rho_E \otimes \text{Tr}_A(M_A(Z_A)\rho_{BA})] \\ &= \text{Tr}_B[\text{Tr}_A(M_A(Z_A)\rho_{BA})], \end{aligned} \quad (5.12)$$

which takes the part of  $\zeta_i$  in transmitted-state BB84. Taking the part of Eq. (5.9) is the conditional probability

$$\begin{aligned} \Pr(X_E, Y_B|Z_A) &\stackrel{\text{def}}{=} \frac{\Pr(X_E, Y_B, Z_A)}{\Pr(Z_A)} \\ &= \frac{\text{Tr}_{EB}\{M_E(X_E)M_B(Y_B)U_{EB}[\rho_E \otimes \text{Tr}_A(M_A(Z_A)\rho_{BA})]U_{EB}^\dagger\}}{\text{Tr}_B[\text{Tr}_A(M_A(Z_A)\rho_{BA})]} \\ &= \text{Tr}_{EB}[M_E(X_E)M_B(Y_B)U_{EB}(\rho_E \otimes \rho_B|_{Z_A})U_{EB}^\dagger], \end{aligned} \quad (5.13)$$

with the conditional density operator

$$\rho_B|_{Z_A} \stackrel{\text{def}}{=} \frac{\text{Tr}_A[M_A(Z_A)\rho_{BA}]}{\text{Tr}_B[\text{Tr}_A(M_A(Z_A)\rho_{BA})]}. \quad (5.14)$$

Entangled-state BB84 requires that the state-event components  $Z_A$  for Alice include four that correspond to the four choices Alice has in transmitted-state BB84. I call these  $Z_{A,i}$ . By virtue of Eqs. (5.12) and (5.13) we arrive at the following

**Proposition:** Any model of entangled-state BB84 of the form of Eq. (5.10) asserts the same joint probabilities relevant to quantum key distribution subject to individual eavesdropping attacks as does the model of transmitted-state BB84 with  $\zeta_i = \Pr(Z_{A,i})$  defined by Eq. (5.12) and with  $\rho_B(i) = \rho_B|_{Z_{A,i}}$  defined by Eq. (5.14).

### Acknowledgments

For very helpful discussions over the past four years, I thank Tai Tsun Wu. This work was supported in part by the Air Force Research Laboratory and DARPA under Contract No. F30602-01-C-0170 with BBN Technologies.

## APPENDIX A: TENSOR PRODUCTS AND PARTIAL TRACES

By a bounded positive operator  $A$  on a Hilbert space  $\mathcal{H}$ , I mean any bounded self-adjoint operator such that  $(\forall |x\rangle \in \mathcal{H}) \langle x|A|x\rangle \geq 0$ . The trace of a positive operator  $A$  on a separable Hilbert space is defined [25] as

$$\text{Tr}(A) = \sum_n \langle \psi_n | A | \psi_n \rangle, \quad (A1)$$

where  $\{\psi_n\}$  is an orthonormal basis. In fact, the value of  $\text{Tr}(A)$  here, which might be infinite, is independent of the choice of basis [11]. As stated in [25] and proved in [11], the trace is invariant under cyclic permutations of the factors of a product:

$$\text{Tr}(ABC) = \text{Tr}(CAB). \quad (A2)$$

For a finite-dimensional vector space, the following discussion is elementary; a start at the more complicated derivations needed for infinite-dimensional, separable Hilbert spaces can be found in Chap. II, Sec. 11 of [11].

The trace of a product of matrices acting on a finite-dimensional vector space  $\mathcal{H}$  is defined by

$$\text{Tr}(MN) = \sum_{j,k} M_{j,k} N_{k,j} = \sum_{j,k} N_{j,k} M_{k,j} = \text{Tr}(NM). \quad (\text{A3})$$

Suppose that  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ . For the tensor product of two vectors  $a \in \mathcal{H}_A$  and  $b \in \mathcal{H}_B$ , with components  $a_J$  and  $b_j$ , respectively, we write the tensor product as a vector  $w \in \mathcal{H}_A \otimes \mathcal{H}_B$  with components  $w_{Jj} = a_J b_j$ . Now let  $M^{(AB)}$  be a matrix operating on vectors of  $\mathcal{H}_A \otimes \mathcal{H}_B$ . A row of such a matrix is specified by a double index such as  $Jj$ , and a column by a double index such as  $Kk$ , so that in the special case  $M^{(AB)} = R^{(A)} \otimes S^{(B)}$ ,  $M_{JjKk}^{(AB)} = R_{JK}^{(A)} S_{jk}^{(B)}$  (where we have assumed  $R^{(A)}$  is a matrix acting on vectors of  $\mathcal{H}_A$  and  $S^{(B)}$  is a matrix acting on vectors of  $\mathcal{H}_B$ ). The partial trace over the  $\mathcal{H}_B$  factor of  $M^{(AB)}$  is defined to be the matrix acting on  $\mathcal{H}_A$  that has as its  $(J, K)$ -th component

$$[\text{Tr}_B(M^{(AB)})]_{JK} = \sum_j M_{JjKj}. \quad (\text{A4})$$

For the full trace over  $\mathcal{H}_A \otimes \mathcal{H}_B$  I write  $\text{Tr}_{AB}$ .

Any matrix  $M^{(AB)}$  can be written as a sum of tensor products, with the result that the properties of partial traces follow from block form of these tensor-product terms. Recall that for finite-dimensional spaces the tensor product of any two matrices  $A$  and  $B$  is a matrix of  $B$ -sized blocks:

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots \\ A_{21}B & A_{22}B & \dots \\ \dots & \dots & \dots \end{bmatrix}, \quad (\text{A5})$$

from which it is obvious that for square matrices  $A$  and  $B$ ,

$$\text{Tr}_B(A \otimes B) = \begin{bmatrix} A_{11}\text{Tr}(B) & A_{12}\text{Tr}(B) & \dots \\ A_{21}\text{Tr}(B) & A_{22}\text{Tr}(B) & \dots \\ \dots & \dots & \dots \end{bmatrix} = [\text{Tr}(B)]A. \quad (\text{A6})$$

Similarly, we have  $\text{Tr}_A(A \otimes B) = [\text{Tr}(A)]B$ , from which it follows immediately that  $\text{Tr}_{AB}(A \otimes B) = [\text{Tr}_A(A)][\text{Tr}_B(B)]$ . Except when computing with matrix components, I drop the superscripts indicating “which space” to subscripts, writing  $M_{AB}$  in place of  $M^{(AB)}$ , etc.

Although the full trace of a product is invariant under a change in the order of the factors, the block form makes apparent that changing the order of factors affects the partial trace of their product; in the general case,

$$\begin{aligned} \text{Tr}_B[(R_A \otimes S_B)(R'_A \otimes S'_B)] &= \text{Tr}_B[(R_A R'_A) \otimes (S_B S'_B)] = [\text{Tr}(S_B S'_B)] R_A R'_A \\ &\neq \text{Tr}_B[(R'_A \otimes S'_B)(R_A \otimes S_B)]. \end{aligned} \quad (\text{A7})$$

It is of course true that for any two matrices  $M$  and  $N$  acting on  $\mathcal{H}_A \otimes \mathcal{H}_B$ , we have

$$\begin{aligned} (\forall M, N) \quad \text{Tr}_A[\text{Tr}_B(MN)] &= \text{Tr}_A[\text{Tr}_B(NM)] \\ &= \text{Tr}_B[\text{Tr}_A(MN)] = \text{Tr}_B[\text{Tr}_A(NM)] = \text{Tr}_{AB}(MN). \end{aligned} \quad (\text{A8})$$

Easily proved are the following facts concerning square matrices, stated with subscripts to indicate the relevant vector spaces,  $\mathcal{H}_A$ ,  $\mathcal{H}_B$ , and  $\mathcal{H}_A \otimes \mathcal{H}_B$ . First, there holds a commutativity relation for partial traces of factors of a certain form:

**Lemma:**

$$(\forall S_B, M_{AB}) \quad \text{Tr}_B[M_{AB}(\mathbf{1}_A \otimes S_B)] = \text{Tr}_B[(\mathbf{1}_A \otimes S_B)M_{AB}]. \quad (\text{A9})$$

*Proof:* Expand any  $M_{AB}$  as a sum of tensor products  $R_A \otimes S_B$ , and observe that for this special case the  $\neq$  of Eq. (A7) becomes equality.  $\square$

The same technique shows

**Lemma:**

$$(\forall \text{ hermitian } S_B, \text{ hermitian } M_{AB}) \quad \text{Tr}_B[M_{AB}(\mathbf{1}_A \otimes S_B)] \text{ is hermitian.} \quad (\text{A10})$$

Again the same technique shows

**Lemma:**

$$\text{Tr}_B[(R_A \otimes \mathbf{1}_B)M_{AB}] = R_A \text{Tr}_B(M_{AB}), \quad (\text{A11})$$

$$\text{Tr}_B[M_{AB}(R_A \otimes \mathbf{1}_B)] = [\text{Tr}_B(M_{AB})]R_A, \quad (\text{A12})$$

from which follows

**Lemma:**

$$(\forall R_A, M_{AB}) \quad \text{Tr}_{AB}[(R_A \otimes \mathbf{1}_B)M_{AB}] = \text{Tr}_A[R_A \text{Tr}_B(M_{AB})]. \quad (\text{A13})$$

Note the stretch of notation so that  $\text{Tr}_A$  is used here for the trace on  $\mathcal{H}_A$ , while it is also used, as above, for the partial trace over the  $A$  factor of  $\mathcal{H}_A \otimes \mathcal{H}_B$ . All these lemmas holds when  $A$  and  $B$  are interchanged; for instance the last lemma becomes:

$$(\forall S_B, M_{AB}) \quad \text{Tr}_{AB}[(\mathbf{1}_A \otimes S_B)M_{AB}] = \text{Tr}_B[S_B \text{Tr}_A(M_{AB})]. \quad (\text{A14})$$

Here is an example of the application to quantum mechanics. Sometimes one wants to compute a conditional density operator of the form

$$\rho_A = \text{Tr}_B(M_A(X)|\psi_{AB}\rangle\langle\psi_{AB}|) \equiv \text{Tr}_A((M_A(X) \otimes \mathbf{1}_B)|\psi_{AB}\rangle\langle\psi_{AB}|), \quad (\text{A15})$$

where  $M_A(X)$  is positive hermitian and thus can be written as a product of its positive square roots  $[M_A(X)]^{1/2}$ . In some cases the calculation is made easier by putting Eq. (A15) in a symmetric form. To this end, interchange  $A$  and  $B$  in Lemma (A9) and change names to obtain

**Lemma:**

$$(\forall R_A, Q_{AB}) \quad \text{Tr}_A[(R_A \otimes \mathbf{1}_B)Q_{AB}] = \text{Tr}_A[Q_{AB}(R_A \otimes \mathbf{1}_B)]. \quad (\text{A16})$$

Apply this with  $R_A$  taken as  $[M_A(X)]^{1/2}$  and with  $Q_{AB}$  taken as  $[M_A(X)]^{1/2}|\psi_{AB}\rangle\langle\psi_{AB}|$  to obtain the symmetrized form

$$\rho_A = \text{Tr}_A\left([M_A(X)]^{1/2}|\psi_{AB}\rangle\langle\psi_{AB}|[M_A(X)]^{1/2}\right). \quad (\text{A17})$$

To deal with partial traces of more complex expressions, a couple of tricks help. The first is a shorthand notation. So far I have written out lots of tensor products of operators in which the operator on one of the factor spaces is the identity operator for that space, as in  $\text{Tr}_B[M_{AB}(\mathbf{1}_A \otimes S_B)]$ , which contains an operator product of the operator  $M_{AB}$  on  $\mathcal{H}_A \otimes \mathcal{H}_B$  times the indicated tensor product  $\mathbf{1}_A \otimes S_B$ . Common in the physics literature and often convenient is a shorthand convention of writing just  $\text{Tr}_B(M_{AB}S_B)$ . This shorthand can be undone by tensoring each operator in such an expression into the identity operators required for the whole expression to make sense.

The second trick is merely to recognize that if  $\mathcal{H}_A$  and  $\mathcal{H}_B$  are distinct factor spaces of a tensor-product space  $\mathcal{H}_{AB}$ , then

$$[M_A, N_B] = [(M_A \otimes \mathbf{1}_B)(\mathbf{1}_A \otimes N_B)] = 0; \quad (\text{A18})$$

that is, operators on distinct factor spaces commute with one another. For example, Lemmas (A9) and (A10) with a swapping of  $A$  and  $B$  become in shorthand notation

$$\text{Tr}_A(M_{AB}R_A) = \text{Tr}_A(R_A M_{AB}) \quad (\text{A19})$$

$$\text{Tr}_A(S_B M_{AB}) = S_B \text{Tr}_A(M_{AB}). \quad (\text{A20})$$

From these equations follows a more complicated relation for operators on a triple tensor product  $\mathcal{H}_E \otimes \mathcal{H}_B \otimes \mathcal{H}_A$ , of use in quantum cryptography:

$$\begin{aligned} \text{Tr}_A[M_E M_B M_A U_{EB} \rho_E \rho_{AB} U_{EB}^\dagger] &= \text{Tr}_A[M_E M_B U_{EB} \rho_E M_A \rho_{AB} U_{EB}^\dagger] \\ &= M_E M_B U_{EB} \rho_E [\text{Tr}_A(M_A \rho_{AB})] U_{EB}^\dagger. \end{aligned} \quad (\text{A21})$$

- 
- [1] F. H. Madjid and J. M. Myers, arXiv:quant-ph/0404113 v2 (2004); *Annals of Physics* (to be published).
  - [2] A. J. Leggett, *Science* **307**, 871 (2005); for a beachhead into more discussion of interpretations, see S. Malin, *Nature Loves to Hide* (Oxford University Press, New York, 2001), Appendix 3; P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement* (Springer-Verlag, Berlin, 1991); J. A. Wheeler and W. H. Zurek, eds., *Quantum Theory and Measurement* (Princeton University Press, Princeton, NJ, 1983).
  - [3] J. M. Myers and F. H. Madjid, in *Quantum Computation and Information*, edited by S. J. Lomonaco, Jr. and H. E. Brandt (American Mathematical Society, Contemporary Mathematics Series, 2002), Vol. 305, pp. 221–244.
  - [4] J. M. Myers and F. H. Madjid, *J. Opt. B: Quantum Semiclass. Opt.* **4**, S109 (2002).
  - [5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
  - [6] S. Wiesner, *SIGACT News* **15**, 78 (1983); C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
  - [7] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, *Phys. Rev. A* **57**, 2383 (1998); B. A. Slutsky, R. Rao, P.-C. Sun, L. Tancevski, and S. Fainman, *Applied Optics* **37**, 2869 (1998).
  - [8] A. N. Kolmogorov, *Foundations of the Theory of Probability*, 2nd English ed. (Chelsea Pub. Co., New York, 1956).
  - [9] G. W. Mackey, *Unitary Group Representations in Physics, Probability, and Number Theory* (Addison-Wesley, Reading, MA, 1978), Chap. 17.
  - [10] W. Rudin, *Real and Complex Analysis*, 3rd ed. (McGraw-Hill, New York, 1987).
  - [11] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932); translated with revisions by the author as *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955).
  - [12] W. Feller, *An Introduction to Probability Theory and Its Applications*, 3rd ed. (Wiley, New York, 1968).
  - [13] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4th ed. (Clarendon Press, Oxford, 1958).
  - [14] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
  - [15] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976); A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
  - [16] M. A. Neumark, *Izv. Akad. Nauk SSSR, Ser. Mat.* **4**, 277 (1940) (Russian-English summary).
  - [17] N. I. Akhiezer and I. M. Glazman, *Theory of Linear Operators in Hilbert Space* (Ungar, New York, 1963), Vol. II, pp. 121–126.
  - [18] S. L. Braunstein and C. M. Caves, *Foundations of Physics Letters* **1**, 3 (1988).
  - [19] J. M. Myers and H. E. Brandt, *Meas. Sci. Technol.* **8**, 1222 (1997).
  - [20] G. Lüders, *Annalen der Physik* **8**, 322 (1951).
  - [21] E. B. Davies, and J. T. Lewis, *Commun. Math. Phys.* **17**, 239 (1970).
  - [22] J. M. Myers, in *Proceedings of SPIE*, Vol. 5815, Quantum Information and Computation III, edited by E. Donkor, A. R. Pirich, H. E. Brandt (SPIE, Bellingham, WA, to be published).
  - [23] J. M. Myers, arXiv:quant-ph/0411107 and quant-ph/0411108, v2 (2005).
  - [24] J. M. Myers, T. T. Wu, and D. S. Pearson, in *Proceedings of SPIE*, Vol. 5436, Quantum Information and Computation II, edited by E. Donkor, A. R. Pirich, H. E. Brandt (SPIE, Bellingham, WA, 2004), pp. 36–47.
  - [25] G. Sewell, *Quantum Mechanics and Its Emergent Macrophysics* (Princeton University Press, Princeton, NJ, 2002).